SC SUNS
South Carolina Department of Education

myscschools.com
South Carolina
Student Unique
Numbering System

South Carolina Department of Education

SCEDS and SUNS

Data Access and Management Policy

South Carolina Department of Education
SCEDS and SUNS
Data Access and Management Policy

I. Introduction/Background

This policy statement pertains to all the data collected and maintained by the South Carolina State Department of Education (SDE) in two information systems: the South Carolina Education Data System (SCEDS) and the Student Unique Numbering System (SUNS). The SCEDS database contains individual student records that will be used for the purpose of collecting data needed for state and federal reporting requirements, including the federal *No Child Left Behind* Act, as well as to meet other data requests from the Department of Education, the South Carolina Education Oversight Committee, the state legislature, and other entities. The SUNS database contains data needed to locate the unique identifier of a student who is currently or has previously been enrolled in a South Carolina public school.

Both the SCEDS and the SUNS are managed by the SDE in accordance with state and federal laws. The Family Educational Rights and Privacy Act of 1974, as amended (FERPA, 34 CFR Part 99), the Individuals with Disabilities Education Act (IDEA, 34 CFR §§ 300.127 and 300.560-300.576), and South Carolina statutes and policies guard the confidentiality and access to students' educational records. All of these laws and policies are essential to maintaining the confidentiality of student records. This policy statement contains information about the procedures that will be used to follow existing laws and ensure the confidentiality of student records maintained in the SCEDS and SUNS databases. It does not expand or in any way change the allowable uses by staff of these systems or the availability of the student records to any other individual.

As established by the SDE, the purpose of South Carolina Education Data System is to reduce data burden and encourage better decision-making by establishing and maintaining a cost-effective method of accessing and transferring accurate and timely education information among school districts and the SDE. Underlying principles of the project include a commitment toward reduction of paper-based reporting, building on existing technologies available to schools, the voluntary adoption of a common basis for facilitating meaningful information exchange between appropriate parties, and greater security of confidential student information.

The SCEDS database contains data on all students in public schools in pre-kindergarten and kindergarten programs and grades one through twelve. Data are obtained from public school districts on a quarterly basis. The database contains minimal data about student participation in state and federal programs for which reporting is required, including, but not limited to, information about English language learners and students in Title I programs and career/technology (Perkins vocational) education. Some assessment data will be stored in this database.

The SUNS contains a selected set of data about individual students that will allow for the assignment of a unique student identifier and that provides a district administrator with the capacity to locate the identifier of a student who has transferred into his/her district from another district within South Carolina. The goal of this system is to maintain a unique identifier for every South Carolina student such that: 1) only one student is ever assigned a particular number; 2) once a student is assigned a number, that number is always associated with that student throughout his or her educational career or until he or she leaves the state; and 3) a student is only assigned one number so that the student is not duplicated in the SCEDS database.

The SCEDS and SUNS are managed by staff in the Office of Technology Services within the Division of Policy, Research, and Technology in the SDE. The Deputy Superintendent of the Division of Policy, Research, and Technology is the designated authority to establish and maintain a system of data protection for the SCEDS and SUNS databases in accordance with the FERPA and other relevant state and federal laws and regulations.

Beginning with the 2003-04 school year, all public school districts must submit their student information system data electronically using the SDE's data extract tool. Beginning in the 2005-2006 school year, each record submitted must contain a unique student identifier.

II. Guiding Principles

The following principles have been used in establishing a Data Access and Management Policy:

- Student information is a valuable asset of the SDE and should be treated as such;
- The SDE manages student information under its control throughout its life cycle, from inception to appropriate destruction;
- The SDE is responsible for controlling access to and use of student information associated with the SCEDS and SUNS databases;
- The SDE is responsible for reviewing and updating policies and regulations covering confidential student information and ensuring that its activities comply with state and federal law; and
- The SDE is responsible for communicating its data collection practices to the providers of the data, including schools and districts.

III. Definitions and Background Information Related to this Policy

South Carolina adheres to the confidentiality requirements of both federal and state laws, including but not limited to FERPA, the Individuals with Disabilities Education Act (IDEA), the Protection of Pupil Rights Amendment (PPRA) and the National School Lunch Act. The following definitions are derived from these laws and other related documents that are relevant to the implementation of the SDE's Data Access and Management Policy associated with the SCEDS and the SUNS.

Privacy refers to an individual's right to freedom from intrusion due to disclosure of

personally identifiable information without consent.

Confidentiality refers to an agency's obligation not to disclose or transmit information about individual students to unauthorized parties. Confidentiality consists of the measures used by an authorized agency to protect how personally identifiable information is collected and maintained and when consent is required to release information.

Personally identifiable information generally includes, but is not limited to: the student's name; the name of the student's parent/guardian; the address of the student or student's family; a personal identifier, such as the state student identifier; personal characteristics or other information that would make the student's identity easily traceable. A small set of this information is essential for assigning identifiers and for identifying students who have transferred from another district within the state or who have returned to the state and already have identifiers. This information will be maintained securely in the SUNS.

Disclosure means to permit access to, revealing, releasing, transferring, or otherwise communicating personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means.

Access means to view, print, download, copy, retrieve data from a computer, computer system, or computer network.

Confidential data means information that would tend, by itself or with other information, to identify particular person(s). Confidential data includes information which is intended for the use of a particular person/group and whose unauthorized disclosure could be prejudicial to the individual it identifies.

IV. Protections

To protect the confidentiality of the individual student information and prevent unauthorized disclosure of data, the SDE has established the following policies and/or practices:

Limit Access to the Student Identification/Locator System

District and School Personnel

The superintendent of a public school district (or his or her designee) is responsible for authorizing access to the SUNS. The superintendent and each authorized staff member must be registered at myscschools.com to receive a unique password and login id. An individual will be granted access to SUNS upon signing an assurance statement, having the signed approval of the superintendent (or his or her designee), and providing the assurance statement to the SDE. The assurance statement must be on file in the SDE before the individual will be granted access to SUNS The level of access, building specific or district wide, to the SUNS will be assigned by the superintendent (or his or her designee) and managed by the SDE through the login and password of the user.

District Access Through Batch Processing or Individual Student Lookup

The SUNS will allow districts to upload a batch file of students for their district, download from the identifier system a batch file of students previously submitted from their district, create a student ID on-line, or use the direct query utility to search for individual students throughout the state. For the purposes of assigning an ID, districts will not be allowed to view or download batch files uploaded by other districts. District staff may only search for students for the purpose of assigning or locating a unique identifier.

State Department of Education Staff Access

Only a limited number of State Department of Education staff have access to the SUNS and to the SCEDS student records. Any SDE employee or agent assigned responsibilities must sign an assurance statement regarding his or her use and the nondisclosure of confidential information. Examples of staff having access are the network administrator and database administrator from the Office of Technology Services, and technology specialists in the Division of Policy, Research and Technology that work directly with districts in implementing and supporting the SUNS and SCEDS databases. The level of access to the system, selected districts/buildings or all records, will depend upon the staff member's responsibilities. Other SDE staff will not have access to the SUNS or SCEDS databases.

Other Access

Other individuals, other than those listed above, will not have access to SUNS or SCEDS except under limited circumstances as enumerated below.

Access Exceptions

Under this Policy, no private or confidential data will be released without the consent of the student or parent except, as may be released, under the following circumstances as stated in 34 CFR Part 99 Final Regulations for FERPA:

1. To teachers and officials of the district in which the student is enrolled when the determination has been made that there are legitimate educational interests, under Section 99.31(a)(1).

2. To school and district personnel when a student is seeking to enroll, under Section 99.31(a)(2).

3. To comply with a lawfully issued subpoena or court order, under Section 99.31(a)(9)(i). The SDE shall make a reasonable effort to notify the parent or student, if eighteen or over, of the subpoena or court order.

4. To educational officials in connection with an audit or evaluation of a federal or state supported education program, under Section 99.32(c)(3).

5. To appropriate parties in connection with an emergency if such knowledge is

necessary to protect the health and safety of the student or other individuals, under Section 99.36(a). In cases of health or safety emergency, the request for release must first be directed to the school district that owns the data. The Deputy Superintendent, under Section 99.36(a), may also convene a committee to evaluate the request to determine whether or not the person who would receive the information is in a position to deal with the emergency and the extent to which time is of the essence.

6. To researchers whose proposals are approved by the Deputy Superintendent, when a clear legitimate educational interest is established, provided that personally identifiable information if discovered is not disclosed to anyone other than the initiator of the request and the data reporting/database manager. A determination of legitimate educational interest is based in part on whether sharing information on a specific person would unfavorably affect that individual's ability to learn and function in the classroom. [Section 99.31(a)(6)]

   Data will be disclosed only on the conditions that: (1) the party to whom the data are released does not disclose the information to any third party without the prior written consent of the Deputy Superintendent, the company who provided the student assessment data (if assessment data are being disclosed), or the school district that owns the data; (2) the data are protected in a manner that does not permit the personal identification of an individual by anyone except the party referenced in the disclosure; and (3) the data are destroyed when no longer needed for the purposes under which the disclosure was granted.

   The Deputy Superintendent of the Division of Policy, Research and Technology will account to the State Superintendent of Education for all disclosures or requests for disclosures. This includes keeping a list of the data, nature, and purposes of the disclosure, and to whom the disclosure was made.

System Security

The SUNS database will be maintained on a server in a locked server room at the SDE. The Office of Technology Services (OTS) Administrator and staff will monitor security notices affecting the system software and will maintain the current software patches for the system components housed at the SDE. OTS staff will monitor the access logs for the database for activity in violation of the Data Access and Management Policy.

A web server used by district personnel to access the identifier and for reporting to the South Carolina Education Data System is located in the Office of Technology Services. The OTS Director and OTS staff will work closely with the Division of Policy, Research, and Technology to ensure appropriate firewall protection and intrusion detection efforts are in place for the system components housed at SDE. The OTS Administrator and OTS staff will monitor security notices affecting the system software and will work to ensure that the current software patches are in place for the system components located at the SDE.

Statistical Security

The SCEDS database will be used to produce summary reports from individual data that relate to groups of students, rather than to single individuals. It will also be linked to other databases to produce summary reports. While it may seem that the use of anonymous aggregated data poses little threat to confidentiality, there are some cases where populations may include only a few individuals. Statistical disclosure is the risk that arises when a population is so narrowly defined that tabulations are apt to produce a reported number small enough to permit the identification of a single individual. In such cases, the Deputy Superintendent will apply ***statistical cutoff procedures*** to ensure that confidentiality is maintained. It is the SDE's intent to avoid the possibility of inadvertently reporting personally identifiable information about any student.

V. Data Use and Release

State and Federal Reporting

A key purpose of the SCEDS database is to provide access to statistical information that improves the education-related decisions of teachers, administrators, policymakers, parents, and other education stakeholders. Private or confidential data on an individual will not be created, collected, stored, used, maintained, or disseminated by the database in violation of federal or state law. If the SDE enters into a contract with a private individual or third party to perform any of the data reporting or database manager functions, that agreement shall require that the data be protected in the same fashion.

The Department will aggregate the individual student data received through SCEDS to complete state and federal reporting requirements including:

- Education Data Exchange Network (EDEN)/Performance Based Data Management Initiative (PBDMI)
- Common Core Data (CCD)
- Condition of Education Report
- State No Child Left Behind Reports (AYP)

Agency Data Sharing

The Department will not grant access to the statewide SUNS to other state agencies. The Department has inter-agency agreements to share limited amounts of data for the benefit of the children of South Carolina that are allowed by law. Other sharing of student data will be prohibited. The Department will comply with requests for individual student data from federal governmental agencies as required by law.

Researchers

The SDE regularly responds to requests for aggregate student data by researchers. However, on occasion, SDE may receive a request for individually identifiable information about students. According to FERPA [Section 99.31(a)(6)], personally identifiable information about students may be released without parental permission to researchers authorized to conduct data processing or research and evaluation studies for or on behalf of the agency. Researchers must submit to the Deputy Superintendent a written request for permission to have access to personally identifiable data that

explains the purpose of the research study, which educational agency or institution the study is being conducted for, and how the researchers will ensure data confidentiality and security. This request will be considered on a case-by-case basis to determine if the request is in accordance with state and federal laws and regulations. The release of student data to researchers outside the SDE is considered a loan of data (i.e., the recipients do not have ownership of the data). Researchers will be required to destroy the data once the research is completed. The SDE reserves the right to charge a reasonable fee for the production of a data file for researchers in accordance with the Freedom of Information policy.

Parents

Upon the request of any individual (or the individual's parent/guardian if the individual is under the age of eighteen) under Section 99.20 of FERPA to gain access to his/her (child's) record contained in the SCEDS or SUNS, the Deputy Superintendent will provide a copy of all or any portion in a comprehensible form. Since the data actually belong to the local education agencies, parents/guardians should seek first to review and amend the student's record through the local education agency.

Under S.C. Code Ann. § 20-7-100, "Each parent, whether the custodial or non-custodial parent of the child, has equal access and the same right to obtain all educational records and medical records of their minor children and the right to participate in their children's school activities unless prohibited by order of the court." To the extent possible, SDE staff will contact the school of record for a child to determine whether there is a court order preventing the release of information to a non-custodial parent.

VI. Improper Disclosure of Student Records

The Deputy Superintendent has the responsibility for determining whether a request for access to the student records constitutes a legitimate request for an appropriate usage of student data. If the request does not meet standards established by the SDE for the lawful release of student data, then the Deputy Superintendent of the Division of Policy, Research and Technology will deny the request.

The Deputy Superintendent is also responsible for determining if personally identifiable information has been inappropriately disclosed by a SDE or school district official or a third party allowed use of the data in violation of this policy. If the disclosure is made by a SDE or school district official in violation of federal law, the official may be subject to a personnel action, including termination (if a SDE employee), or suspension of login privileges. If an improper disclosure is made by someone other than a SDE or school district official, then the parties will not have access to any data reporting/database information for five years as required by FERPA. In addition, all violations will be reported to the appropriate federal and state enforcement agencies.

VII. Ownership of the Data

School districts or other primary sources of the data that are located in the SUNS and SCEDS databases are the originators and owners of those data. The Deputy

Superintendent functions as the custodian of the data in the SDE. In order to protect the data in its custody, the SDE has established this policy which is implemented by the Deputy Superintendent. The policy ensures that all data are securely maintained with safeguards on all personally identifiable information in the databases.

SUNS System Assurance Statement

Individual student information contained in the SDE's SUNS is collected for the purpose of generating unique student identification numbers. The data are protected by state and federal laws and must be maintained in a confidential manner at all times.

As an employee of a local school district or the SDE that has access to records in the SUNS, you are required to maintain this information in a confidential manner. The unauthorized access to, modification, deletion or disclosure of information from the SUNS may compromise the integrity of the system, violate individual student rights of privacy, and/or constitute a punishable act and subject the employer to a loss of federal funds.

Unauthorized viewing, reproduction/copying, and/or distribution of any student record or information outside the intended and approved use of the SUNS are strictly prohibited. Users violating the authorized use of the SUNS will lose access privileges to the system. Illegal access or misuse of this information may also be cause for disciplinary action, including termination.

I have received and read the SDE's Data Access and Management Policy Statement for the South Carolina South Carolina Education Data System and the Student Unique Numbering System.
.

I acknowledge and agree to the above requirements.

District/Organization Name: _____

Employee Signature: _____

Employee Phone Number:_____

Date: _____

Superintendent or Designee Signature: _____

SCEDS System Assurance Statement

Individual student information contained in the SDE's South Carolina Education Data System (SCEDS) is collected for the purpose of collecting data needed for state and federal reporting requirements. The data are protected by state and federal laws and must be maintained in a confidential manner at all times.

As an employee of the SDE that has access to records in the SCEDS, you are required to maintain this information in a confidential manner. The unauthorized access to, modification, deletion or disclosure of information from the SCEDS may compromise the integrity of the system, violate individual student rights of privacy, and/or constitute a punishable act and subject the employer to a loss of federal funds.

Unauthorized viewing, reproduction/copying, and/or distribution of any student record or information outside the intended and approved use of the SCEDS are strictly prohibited. Users violating the authorized use of the SCEDS will lose access privileges to the system. Illegal access or misuse of this information may also be cause for disciplinary action, including termination.

I have received and read the SDE's Data Access and Management Policy Statement for the South Carolina South Carolina Education Data System and the Student Unique Numbering System.

I acknowledge and agree to the above requirements.

District/Organization Name: _____

Employee Signature: _____

Employee Phone Number: _____

Date: _____

Superintendent or Designee Signature: _____

Date: _____